Western Number Theory Problems, 17 & 19 Dec 2012

Edited by Gerry Myerson

for distribution prior to 2013 (Asilomar) meeting

Summary of earlier meetings & problem sets with old (pre 1984) & new numbering.

1967 Berkeley	1968 Berkeley	1969 Asilomar	
1970 Tucson	1971 Asilomar	1972 Claremont	72:01–72:05
1973 Los Angeles	73:01–73:16	1974 Los Angeles	74:01–74:08
1975 Asilomar	75:01–75:23		
1976 San Diego	1–65 i.e., 76:01–76:65		
1977 Los Angeles	101–148 i.e., 77:01–77:48		
1978 Santa Barbara	151–187 i.e., 78:01–78:37		
1979 Asilomar	201–231 i.e., 79:01–79:31		
1980 Tucson	251–268 i.e., 80:01–80:18		
1981 Santa Barbara	301–328 i.e., 81:01–81:28		
1982 San Diego	351–375 i.e., 82:01–82:25		
1983 Asilomar	401–418 i.e., 83:01–83:18		
1984 Asilomar	84:01–84:27	1985 Asilomar	85:01–85:23
1986 Tucson	86:01–86:31	1987 Asilomar	87:01–87:15
1988 Las Vegas	88:01–88:22	1989 Asilomar	89:01–89:32
1990 Asilomar	90:01–90:19	1991 Asilomar	91:01–91:25
1992 Corvallis	92:01–92:19	1993 Asilomar	93:01–93:32
1994 San Diego	94:01–94:27	1995 Asilomar	95:01–95:19
1996 Las Vegas	96:01–96:18	1997 Asilomar	97:01–97:22
1998 San Francisco	98:01–98:14	1999 Asilomar	99:01–99:12
2000 San Diego	000:01–000:15	2001 Asilomar	001:01–001:23
2002 San Francisco	002:01–002:24	2003 Asilomar	003:01–003:08
2004 Las Vegas	004:01–004:17	2005 Asilomar	005:01–005:12
2006 Ensenada	006:01–006:15	2007 Asilomar	007:01–007:15
2008 Fort Collins	008:01–008:15	2009 Asilomar	009:01–009:20
2010 Orem	010:01–010:12	2011 Asilomar	011.01–011.16
2012 Asilomar	012:01–012:17		

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Department of Mathematics,
Macquarie University,
NSW 2109 Australia
gerry.myerson@mq.edu.au
Australia-2-9850-8952 fax 9850-8114

Problems proposed 17 and 19 December 2012

012.01 (Russell Jay Hendel). Let

$$\alpha_{2,3} = \sum_{n=0}^{\infty} \frac{1}{3^n 2^{3^n}}$$

Stoneham proved $\alpha_{2,3}$ is normal in base 2 (R. Stoneham, On absolute (j, epsilon)-normality in the rational fractions with applications to normal numbers, Acta Arithmetica 22 (1973) 277–286). It is not normal in base 6, where it has long strings of zeros (see D. H. Bailey, A non-normality result, http://www.davidhbailey.com/dhbpapers/alpha-6.pdf). Is it normal in base 6 if you "ignore the zeros"? That is, if you delete the long strings of zeros from the base 6 expansion of $\alpha_{2,3}$, is the resulting number normal in base 6?

012.02 (Richard Guy via Colin Weir). Let p be a prime, $p \equiv 3 \pmod 4$, and let the negative continued fraction for $\sqrt{p}$ be $[a_0; \dot{a}_1, \ldots, \dot{a}_r]$. Let $m = (1/3)(a_1 + \cdots + a_r) - r$. Let $h(D)$ be the class number of $\mathbf{Q}(\sqrt{D})$. Is it true that

$h(-p)h(p) - m \equiv 0 \pmod{16}$ if $h(p) \equiv \pm 1 \pmod 8$ and

$h(-p)h(p) - m \equiv 8 \pmod{16}$ if $h(p) \equiv \pm 3 \pmod 8$?

It is a theorem of Zagier (Nombres de classes et fractions continues, Astérisque 24–25 (1975) 81–97) that if $h(p) = 1$ then $h(-p) = m$.

012.03 (David Bailey). Let

$$\phi(r_1, \ldots, r_n) = \frac{1}{\pi^2} \sum_{m_i \text{ odd}} \frac{(\cos m_1 r_1 \pi) \cdots (\cos m_n r_n \pi)}{m_1^2 + \cdots + m_n^2}$$

Prove that if $r_1, \ldots, r_n$ are rational then $\phi(r_1, \ldots, r_n) = (1/\pi) \log \alpha$ for some algebraic number α. Note: this has been proved for $n = 2$. See
http://www.davidhbailey.com/dhbpapers/PoissonLattice.pdf

012.04 (David Bailey). With the notation of the previous problem, and $d = \prod^k p_i^{e_i}$, is it true that the degree of $\exp(8\pi\phi_2(1/d, 1/d))$ is

$$4^{k-1} \prod_i p_i^{2(e_i - 1)} m(p_i)$$

where $m(2) = 1/2$, $m(4k+1) = 4k^2$, $m(4k+3) = (2k+1)(2k+2)$?

012.05 (Kjell Wooding). Given sets A and B of points in $\mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$, how can one find, efficiently, the points a in A and b in B that minimize the distance from a to b? That is, if we write $\overline{r}$ for the least absolute residue of r modulo n, we want to minimize $(\overline{x - x'})^2 + (\overline{y - y'})^2$ over all (x, y) in A and (x', y') in B.

Remark: Suppose A and B have roughly m members each. The naive algorithm of computing all pairwise distances requires m^2 comparisons.

Solution: (Colin Weir) Keep two lists of points, sorted by first and second co-ordinate, respectively, and proceed iteratively as new points in the sets are considered. It should be possible to bound how far you need to look around each new point based on the current closest point, so this should improve on m^2.

Solution: (Albert Bush) For the Euclidean plane version of this problem, you can cut the plane in half, solve the problem in each half, and then check across the boundary (where Colin Weir's idea can be used). Doing this recursively should get us to $O(m \log m)$ comparisons. A similar idea could work on $\mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$.

012.06 (Ron Graham, via Steve Butler, via Albert Bush). Given a 3-coloring of $S = \{1, 2, \ldots, n\}$, a *rainbow 3-term arithmetic progression* is a triple $(x, x+d, x+2d)$ of elements of S with all distinct colors.

a) Is it true that the coloring to maximize the number of rainbow 3-APs is R, G, B, R, G, B, R, G, B, ...? (that is, the coloring where terms have the same color if and only if they are congruent modulo 3).

b) It seems that adding a 4th color does not result in an asymptotic increase in the number of rainbow 3-APs, but adding a 5th color does. Why is this?

Remark: A paper on related problems is available at
http://orion.math.iastate.edu/butler/papers/unrolling.pdf

012.07 (Douglas Stones via Gerry Myerson). Are there 6 distinct positive integer base 10 palindromes in geometric progression? There are 5;

$$1, 11, 121, 1331, 14641$$

and the related 11×101^n, 111×1001^n and so on for $0 \leq n \leq 4$. Other examples are 147741×91^n and 1478741×91^n, $0 \leq n \leq 4$. There are no examples of palindromic ar^n, $0 \leq n \leq 5$, for $a, r \leq 10^7 + 1$.

012.08 (Zander on math.stackexchange.com via Gerry Myerson). Is it true that every prime $p > 20627$ can be written as

$$p = w^2 + cw + d$$

with w, c, and d positive integers and cd a cube? This is related to the family of elliptic curves

$$y^2 = x^3 + \frac{1}{4} + \frac{p}{c^2}$$

where $y = (w/c) + (1/2)$, $x = -a/c$, $cd = a^3$ (thanks to Renate Scheidler for filling in the details).

012.09 (Robert Akscyn). For p prime define $R(h, p)$ by

$$R(h, p) = \#\{\, n \leq h : \text{the least prime dividing } n \text{ is at least } p \,\}$$

Let $p < q$ be consecutive primes, and note that $R(q-1, p) = 1$. How can we resolve the recurrence

$$R(h, q) = R(h, p) - R(h/p, p) - R(q-1, p)$$

012.10 (Bobby Grizzard). Are there infinitely many primes p of the form

$$p = \frac{q^n - 1}{q - 1}$$

with $q = \ell^f$ and ℓ prime?

Remark: Presumably, the answer is yes; for example, standard conjectures imply that there are infinitely many primes q for which $q^2 + q + 1$ is prime. Proving anything may be a different matter. Some examples are tabulated in Harvey Dubner, Generalized repunit primes, Math. Comp. 61 (1993), no. 204, 927–930, MR1185243 (94a:11009).

012.11 (Mits Kobayashi). Are there any examples of

$$\sigma(p^e) = \sigma(q^f)$$

with p and q distinct primes, $e > 1$, $f > 1$, other than $\sigma(5^2) = \sigma(2^4)$?

Remark: Problem D10 in UPINT mentions "the conjecture of Goormaghtigh, that the only solutions of

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}$$

with $x, y > 1$ and $n > m > 2$ are $\{x, y, m, n\} = \{5, 2, 3, 5\}$ and $\{90, 2, 3, 13\}$," and gives references to partial results. The review by Nikos Tzanakis of Maohua Le, On the Diophantine equation $(x^3 - 1)/(x - 1) = (y^n - 1)/(y - 1)$, Trans. Amer. Math. Soc. 351 (1999), no. 3, 1063–1074, MR1443198 (99e:11033), says "the author proves that the only solutions (x, y, n) to the title equation when y is a power of a prime are $(5, 2, 5)$ and $(90, 2, 13)$."

012.12 (John Brillhart). What do you do when you have two different ways to estimate the probability of an event? For example, suppose that you know the probability of n being prime is at least 1/4, but you also may know how many primes there are in some interval containing n.

Remarks: 1. The paper Beauchemin, Brassard, Crépeau, Goutier, Two observations on probabilistic primality testing, Advances in cryptology—CRYPTO '86 (Santa Barbara, Calif., 1986), 443–450, Lecture Notes in Comput. Sci., 263, Springer, Berlin, 1987, MR0907106 (89c:11180), has some observations that seem to be relevant.

2. (Russell Hendel) Since you have uncertainty not only about the event but about which distribution to use, you could simply use a compound distribution approach in which each "method" is assigned a probability. Your "revised" uncertainty of the event is then the compound probability. There are in fact some theorems on expectations and variances on conditioned distributions. $(E(X) = E(E(X|Y)$ and $Var(X) = E(Var(X|Y)) + Var(E(X|Y)))$

3. (Rob Akscyn) One way to address the situation is the view that probability is a measure of ignorance. It is a property of the observer — not the system. To expand on this, many tend to confound the notion of probability and reality. If (as I submit) in many cases/scenarios that probability is really a measure of the state of the observer (what it believes about the system) then it is easier to see how two measures of probability about the same system can be different from one another (as they reflect the idiosyncracies of the observers/models/...).

012.13 (Colin Weir). Given $b_0, b_1, \ldots, b_r$, what properties of the number α with continued fraction expansion $[b_0; \dot{b}_1, \ldots, \dot{b}_r]$ can we deduce without calculating the number? For example, what properties of $b_0, b_1, \ldots, b_r$ would imply $\alpha = (a + b\sqrt{D})/c$ with $D \equiv 1 \pmod 4$? or $D \equiv 0 \pmod 2$? or restrictions on the size of D?

Remark: Russell Hendel suggests consulting Edward B. Burger, A tail of two palindromes, Amer. Math. Monthly 112 (2005) 311-321, MR 2005i:11011, and C. Kimberling, Initialized continued fractions and Fibonacci numbers, in Proceedings of the Twelfth International Conference on Fibonacci Numbers and Their Applications, Congressus Numerantium 200 (2010) 269-284, MR2597725.

012.14 (Mark Kozek). Find a composite N, $\gcd(N, 10) = 1$, such that if you replace any two adjacent digits of N with any pair $00, 01, \ldots, 99$ you get a composite number.

Remarks: 1. For the one-digit replacement problem, see Filaseta, Kozek, Nicol, Selfridge, Composites that remain composite after changing a digit, J. Comb. Number Theory 2 (2010), no. 1, 25–36 (2011), MR2895985 (2012m:11008).

2. For the 2-digit problem, examples are known in bases 2 and 3 (work by Kozek and students, in preparation for publication).

012.15 (Mark Kozek). A *Riesel number* is an odd integer r such that $r2^n - 1$ is composite for all positive integers n. A *Sierpiński number* is an odd integer s such that $s2^n + 1$ is composite for all positive integers n. Given a digit d coprime to 10, can we construct a sequence $r, rd, rdd, rddd, \ldots$ or a sequence $r, dr, ddr, dddr, \ldots$ in which every member is a Riesel number? Can we construct a sequence $s, sd, sdd, sddd, \ldots$ or a sequence $s, ds, dds, ddds, \ldots$ in which every member is a Sierpiński number?

Remark: Introduce the notation $r(0) = r$, $r(1) = rd$, $r(2) = rdd$, and so on. It is known that there is a number r such that $r(6912k)$ is a Riesel number for $k = 0, 1, 2, \ldots$. A similar result can be proved for Sierpiński numbers (work by Kozek and students, in preparation for publication).

012.16 (Rob Akscyn). The Euler sieve

http://en.wikipedia.org/wiki/Sieve_of_Eratosthenes#Euler.27s_Sieve

is a variant on the sieve of Eratosthenes. Where does it appear in Euler's work?

Remarks: 1. The Euler Archive at http://www.math.dartmouth.edu/˜euler/ may be useful.

2. Ed Sandifer wrote about 70 "How Euler Did It" columns for the MAA — perhaps it's in one of his columns. If not, perhaps he knows about it anyway.

012.17 (Hee-sung Yang). Let $\sigma^*(n)$ be the sum of the unitary divisors of n (the divisors d relatively prime to n/d). Let $s^*(n) = \sigma^*(n) - n$, and let U^* be the numbers not of the form $s^*(n)$. Let $s(n) = \sigma(n) - n$, U the numbers not of the form $s(n)$. Let $s_\phi(n) = n - \phi(n)$, Φ the numbers not of the form $s_\phi(n)$.

a) The lower density of U^* is positive (Pomerance and Yang, Variant of a theorem of Erdős on the sum-of-proper-divisors function,
http://www.math.ucla.edu/˜hyang/publications/varianterdos.pdf). Does the density of U^* exist?

b) Almost all odd numbers are of the form $s(n)$ (this follows from work of Montgomery and Vaughan on the exceptional set in Goldbach's problem). Are a positive proportion of even numbers of the form $s(n)$?

c) Are a positive proportion of even numbers of the form $s_\phi(n)$?

d) Is the lower density of Φ positive?